This listing of claims will replace all prior versions, and listings, of claims in the application:

The Status of the Claims

1. (Currently Amended) A method of receiving a password, the method comprising:

receiving a password routine, the password routine being digitally signed using a private key;

authenticating the password routine using a public key associated with the private key;

storing the password routine in a first area of a memory device, the first area of the memory device being unavailable to a memory management unit, the memory device including a second area, the second area being available to the memory management unit;

executing a monitor routine at a first privilege level to secure a pre-boot environment; and

executing the password routine at a second privilege level ~~in a pre-boot environment~~ in the pre-boot environment to receive the password, wherein the first and second privilege levels are different.

2. (Original) A method as defined in claim 1, further comprising executing a non-trusted device driver in the pre-boot environment.

3. (Original) A method as defined in claim 2, wherein the non-trusted device driver is only executed if the password matches a password stored in the first area of the memory device.

4. (Original) A method as defined in claim 3, wherein the non-trusted device driver is stored in the second area of the memory device.

5. (Original) A method as defined in claim 1, wherein executing the password routine comprises executing the password routine using a processor in a secure mode, the secure mode being a hardware feature of the processor.

6. (Original) A method as defined in claim 5, wherein the secure mode limits the use of input hardware.

7. (Original) A method as defined in claim 6, wherein the secure mode limits the use of output hardware.

8. (Original) A method as defined in claim 1, wherein the password routine calls a trusted graphics routine, the trusted graphics routine being digitally signed.

9. (Original) A method as defined in claim 8, wherein the trusted graphics routine calls a trusted display driver, the trusted display driver being digitally signed.

10. (Original) A method as defined in claim 1, wherein the password routine calls a trusted keyboard driver, the trusted keyboard driver being digitally signed.

11. (Original) A method as defined in claim 1, wherein the password comprises a basic input output system (BIOS) password.

12. (Currently Amended) An apparatus to execute a trusted software program in a pre-boot environment, the apparatus comprising:

a memory device including a first memory portion and a second memory portion, the first memory portion storing the trusted software program;

a memory management unit operatively coupled to the memory device, the memory management unit being unable to access the first memory portion, the memory management unit being able to access the second memory portion; and

a processor operatively coupled to the memory device, the processor to execute the trusted software program in the pre-boot environment, wherein the processor is configured to secure an address of the memory device to prevent another software program from accessing the first memory portion during execution of the trusted software program.

13. (Original) An apparatus as defined in claim 12, further comprising a non-trusted software program stored in the second memory portion.

14. (Original) An apparatus as defined in claim 13, wherein the processor executes the non-trusted software program in the pre-boot environment.

15. (Original) An apparatus as defined in claim 12, wherein the trusted software program comprises a hardware driver.

16. (Original) An apparatus as defined in claim 15, wherein the hardware driver comprises a keyboard driver.

17. (Original) An apparatus as defined in claim 15, wherein the hardware driver comprises a display driver.

18. (Original) An apparatus as defined in claim 12, wherein the trusted software program comprises a graphical user interface display routine.

19. (Original) An apparatus as defined in claim 12, wherein the trusted software program comprises a password collection routine.

20. (Original) An apparatus as defined in claim 12, wherein the processor includes a secure mode that limits the use of input hardware and output hardware connected to the processor.

21. (Original) An apparatus as defined in claim 20, wherein the processor executes the trusted software program in the pre-boot environment while the processor is in the secure mode.

22. (Currently Amended) An apparatus to collect a password in a pre-boot environment, the apparatus comprising:

a memory device including a first memory portion and a second memory portion, the second memory portion storing a keyboard driver, a display driver, graphics routine, and a password collection routine;

a memory management unit operatively coupled to the memory device, the memory management unit being able to access the first memory portion, the memory management unit being unable to access the second memory portion; and

a processor operatively coupled to the memory device, the processor to execute a monitor routine at a first privilege level to secure the pre-boot environment and to execute the keyboard driver, the display driver, the graphics routine, and the password collection routine at a second privilege level in the pre-boot environment to collect the password in the pre-boot environment, wherein the first and second privilege levels are different.

23. (Original) An apparatus as defined in claim 22, wherein the keyboard driver, the display driver, the graphics routine, and the password collection routine are each authenticated using a digital signature.

24. (Original) An apparatus as defined in claim 22, wherein the processor includes a secure mode that limits the use of input hardware and output hardware connected to the processor.

25. (Original) An apparatus as defined in claim 24, wherein the processor executes the keyboard driver, the display driver, the graphics routine, and the password collection routine in the pre-boot environment while the processor is in the secure mode.

26. (Currently Amended) A machine readable medium storing instructions structured to cause a machine to:

receive a password routine, the password routine being digitally signed using a private key;

authenticate the password routine using a public key associated with the private key;

store the password routine in a first area of a memory device, the first area of the memory device being unavailable to a memory management unit, the memory device including a second area, the second area being available to the memory management unit; ~~and~~

execute the password routine in a pre-boot environment to receive the password; and

secure an address of the memory device to prevent another software program from accessing the first area of the memory device during execution of the password routine.

27. (Original) A machine readable medium as defined in claim 26, wherein the instructions are structured to cause the machine to executing a non-trusted software routine in the pre-boot environment, the non-trusted software routine being stored in the second area of the memory device.

28. (Original) A machine readable medium as defined in claim 27, wherein the non-trusted software routine comprises a legacy driver.